南明离火
移动应用检测平台

ANDROID 静态分析报告

短信宝典 · V2.1.0

分析日期: 2025-05-10 09:43:28

应用概览

文件名称:	短信宝典 v2.1.0.apk
文件大小:	10.74MB
应用名称:	短信宝典
软件包名:	net.joydao.spring2011
主活动:	.LoadingActivity
版本号:	2.1.0
最小SDK:	8
目标SDK:	18
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	37/100 (高风险)
跟踪器检测:	3/432
杀软检测:	16 个杀毒软件报毒
MD5:	b0a5a1d9eaf6423b0d8fef0c3b986d82
SHA1:	dda9525592641a22a85c8ada7f15df071300a2e0
SHA256:	00d90efadf37f6da1a9d85a5b6e3c23c409d8afaf7f4951062f33478c79408f

分析结果严重性分布

高危	中危	信息	安全	关注
5	15	1	0	3

四大组件导出状态统计

Activity组件：4个，其中export的有： 1个
Service组件：4个，其中export的有： 0个
Receiver组件：2个，其中export的有： 2个

Provider组件：1个，其中export的有： 1个

应用签名证书信息

二进制文件已签名
v1 签名: True
v2 签名: False
v3 签名: False
v4 签名: False
主题: C=CN, ST=Guangdong, L=Shenzhen, O=www.joydao.net, OU=www.joydao.net, CN=joydao
签名算法: rsassa_pkcs1v15
有效期自: 2010-04-02 01:47:29+00:00
有效期至: 2065-01-03 01:47:29+00:00
发行人: C=CN, ST=Guangdong, L=Shenzhen, O=www.joydao.net, OU=www.joydao.net, CN=joydao
序列号: 0x4bb54cb1
哈希算法: sha1
证书MD5: 8483e0c6ffb2826db0d39727969cc8ee
证书SHA1: 362aa4dbb63c005fa33019fcb4263efab1eb04bf
证书SHA256: 4d31762526e8a79d754dbb9197d326ae6abf21bb3ae60efd2ecbb679a787d610
证书SHA512:
d110b9cb2f44aea69f008ebb389f9335814923dbc1fb051dbc06d512f288dfd84f33885a452f67fb2b80874c5709373c8b5ddd864a2c12d88cb5c1fa7ecb45f7

找到 1 个唯一证书

权限声明与风险分级

权限名称	安全等级	权限内容	权限描述
android.permission.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户粗略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
android.permission.ACCESS_NETWORK_STATE	普通	获取网络状态	允许应用程序查看所有网络的状态。
android.permission.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
android.permission.SET_WALLPAPER	普通	设置壁纸	允许应用程序设置壁纸。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.ACCESS_WIFI_STATE	普通	查看Wi-Fi状态	允许应用程序查看有关Wi-Fi状态的信息。
android.permission.READ_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储。

android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
com.android.launcher.permission.INSTALL_SHORTCUT	签名	创建快捷方式	这个权限是允许应用程序创建桌面快捷方式。
android.permission.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
android.permission.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
android.permission.VIBRATE	普通	控制振动器	允许应用程序控制振动器，用于消息通知振动功能。
android.permission.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全合规分析

高危: **1** | 警告: **0** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序使用代码签名证书进行签名
应用程序容易受到 Janus 漏洞的影响	高危	应用程序使用 v1 签名方案进行签名。如果仅使用 v1 签名方案进行签名，则在 Android 5.0-8.0 上容易受到 Janus 漏洞的影响。在使用 v1 和 v2/v3 方案签名的 Android 5.0-7.0 上运行的应用程序也容易受到攻击。

Manifest 配置安全分析

高危: **1** | 警告: **5** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用数据存在泄露风险 未设置[android:allowBackup]标志	警告	建议将 [android:allowBackup] 显式设置为 false。默认值为 true，允许通过 adb 工具备份应用数据，存在数据泄露风险。
2	Activity (.MainActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
3	Activity (.MessagesActivity) 未受保护。 存在 intent-filter。	警告	检测到 Activity 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity 被显式导出，存在安全风险。

4	Broadcast Receiver (.MessageReceiver) 未受保护。存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
5	Content Provider (.provider.MessageProvider) 未受保护。[android:exported=true]	警告	检测到 Content Provider 已导出，未受任何权限保护，任意应用均可访问。
6	Broadcast Receiver (net.youmi.android.AdReceiver) 未受保护。存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。

代码安全漏洞检测

高危: **3** | 警告: **8** | 信息: **1** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	应用程序记录日志信息,不得记录敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
2	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
3	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限
4	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限
5	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限

6	使用弱加密算法	高危	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
7	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
8	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
9	文件可能包含硬编码的敏感信息，如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
10	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
11	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
12	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED(裁剪符号表)
1	armeabi/libbspatch.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出。	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	True info 符号被剥离

本报告由南明离火移动安全分析平台生成

应用行为分析

编号	行为	标签	文件

00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00137	获取设备的最后已知位置	位置 信息收集	升级会员：解锁高级权限
00115	获取设备的最后已知位置	信息收集 位置	升级会员：解锁高级权限
00016	获取设备的位置信息并将其放入 JSON 对象	位置 信息收集	升级会员：解锁高级权限
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
00078	获取网络运营商名称	信息收集 电话服务	升级会员：解锁高级权限
00171	将网络运算符与字符串进行比较	网络	升级会员：解锁高级权限
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00162	创建 InetSocketAddress 对象并连接到它	socket	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	升级会员：解锁高级权限
00067	查询IMSI号码	信息收集	升级会员：解锁高级权限
00031	检查当前正在运行的应用程序列表	反射 信息收集	升级会员：解锁高级权限
00034	查询当前数据网络类型	信息收集 网络	升级会员：解锁高级权限
00035	查询已安装的包列表	反射	升级会员：解锁高级权限
00023	从当前应用程序启动另一个应用程序	反射 控制	升级会员：解锁高级权限
00112	获取日历事件的日期	信息收集 日历	升级会员：解锁高级权限

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	7/30	android.permission.ACCESS_COARSE_LOCATION android.permission.READ_PHONE_STATE android.permission.SET_WALLPAPER android.permission.ACCESS_FINE_LOCATION android.permission.RECEIVE_BOOT_COMPLETED android.permission.GET_TASKS android.permission.VIBRATE
其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE com.android.launcher.permission.INSTALL_SHORTCUT android.permission.CHANGE_WIFI_STATE

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

恶意域名威胁检测

域名	状态	中国境内	位置信息
m.310win.com	安全	是	**IP地址:** 106.11.130.216 **国家:** 中国 **地区:** 广东 **城市:** 肇庆 **纬度:** 23.051760 **经度:** 112.459717 **查看:** 高德地图
w.m.taobao.com	安全	是	**IP地址:** 106.11.130.216 **国家:** 中国 **地区:** 广东 **城市:** 深圳 **纬度:** 22.545673 **经度:** 114.068108 **查看:** 高德地图
www.joydao.net	安全	是	**IP地址:** 180.153.100.46 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• 223.5.5.5	net/youmi/android/a/b/i/c.java

• http://www.joydao.net	net/joydao/spring2011/BaseActivity.java
• http://m.310win.com/?cid=308	net/joydao/spring2011/MainActivity.java
• 10.0.0.172	net/youmi/android/a/b/i/i.java
• http://openapi.baidu.com/public/2.0/bmt/translate?client_id=illkzwrgqlh2q6s6lwse0mbw&q=	net/joydao/spring2011/util/TranslateUtils.java
• http://w.m.taobao.com/ • http://w.m.taobao.com/api/ • http://w.m.taobao.com/api/r? • http://w.m.taobao.com/api/q?	com/alimama/mobile/csdk/umupdate/b/a.java
• 210.72.145.44 • 66.92.68.246 • 129.7.1.66 • 128.118.46.3 • 130.149.17.21 • 203.117.180.36 • 133.100.11.8 • 64.236.96.53 • 18.145.0.30 • 133.100.9.2 • 131.107.1.10 • 137.92.140.80	net/youmi/android/onlineconfig/ntp/a.java
• 10.0.0.172	u/aly/t.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
bspatch	Google	bspatch library for applying delta patches.
友盟推送	Umeng	基于友盟+全域数据建立精准的消息推送平台，为开发者提供更灵活、更智能、更有效的消息推送方案，有效提升用户粘性，提高 App 活跃度。
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。

第三方追踪器检测

名称	类别	网址
Alimama (formerly AdsMogo)	Advertisement	https://reports.exodus-privacy.eu.org/trackers/338
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119
Umeng Feedback		https://reports.exodus-privacy.eu.org/trackers/120

敏感凭证泄露检测

可能的密钥
友盟统计的=> "UMENG_CHANNEL" : "wandoujia"
友盟统计的=> "UMENG_APPKEY" : "4d40dde83ea7a36f6c0792d2"
0a4144490c4b1b441603124a5f42484d09115d5b4c0a00401d17554d0d590b16
0256584b1f5e435f0d1c50564c5b5e5645014c405c5f0f5b085f
1c740c5146585e531f050417051e4f12461512715307505c
C306239E75034d979DB1957AC06E4612
49205a5c460d58511b54564554494c410e0a554556070558514e4d7977767b367701225002770a5063500407509e2006095c0d740f07727472766749
929bb76e8110d1a70260af57b446ebc
0a4144490c4b1b560d11481359590a1a1f0b455f0b4a0b51464e10514b4d0b123b4c4507
0a4144490c4b1b500e0d0405541b1f4d0714591c0c01111b411507164b41514d07565b05
CBD2998A3D5A4744BF128B91E1410DEA
0a4144490c4b1b560d11481359590a1a1f0b455f0b4a0b51464e10514b500776
0a4144490c4b1b500e0d0405541b1f4d0714591c0c01111b45000a0e4b560d114b4f064c1f5d453e1d4005
545c094f4959110f5e4b025d194a1555444c4c42590a585b5754
0a4144490c4b1b441603124a5f42484d09115d5b4c0a00401d0016124b41514d005c433c104451004c55
0a4144490c4b1b441603124a5f42484d09115d5b4c0a00401d000911 b41517d145746
0a4144490c4b1b441603124a5f42484d09115d5b4c0a00401d1212c3101814514b5a5a0d03
4d480b14580d560751585c
iVBORw0KGgoAAAANSUhEUgAAAEYAAABGBAMAAACDAP+3AAAAIVBMVEUAAAD9pxn9pxn9pxn9pxn9pxn9pxn9pxn9pxn9pxlbgtlYAAAA CnRSTlMAoPAwEdNykLBACW4d5gAAAIBJREFUSMftzaENgDAQheESCCRV6DosijABQzAFmgGYgQ0qMG9KeA2poncWcc/en++czcZ5WGONNdak nVNuuv07acYIn4HaUg0PqakQC79mrQ81uBeamhCbjowAsdnICNDTtGQE6PAQGULRQ2YIBcgMIYCMAoGMApHRIDIaNDh9i7P9dzdh+TgsiueH WgAAAABJRU5ErkJggg==
0a4144490c4b1b500e0d04055 1b1f4d0714591c0c01111b45000a0e4b560d114b4f064c025141
e298a29c3e4ed1313f3a82588d004ffd
0a4144490c4b1b561 1103104b1b1f5905005e1c0c01111b5d0700071618030d1716590a1640464f50440c5c
0e154048 e4d1e471a495844580f4c5b041116454509121f550e101742001b04405e13
0e1540480e4d1e545b43195642481b5a140850185b03121f56000d5651401b100719160647
CEF2F5AD195541b7AD8E8B0E2F44B42D

DD2E1AD5215B757A908C48D980702694
e298a29c3e4ed1313f3a82588d004ffa
0a4144490c4b1b500e0d0405541b1f4d0714591c0c01111b411507164b41514d0d575c17
0e1540480e4d1e471a495844580f4c5b041116454509121f550e101742001b04505a0f
0a4144490c4b1b56174c1f0b4d580f1a0801441d0d020351404e070d1718110e0d5c5b174b5c410c54
0a4144490c4b1b560d11481359590a1a1f0b455f0b4a0b51464e10514b450713
0a4144490c4b1b500e0d0405541b1f4d0714591c0c01111b411507164b560d114b4f064c155a46
0e1540480e4d1e471a495844580f4c5b0411165956020f491b000c4b1b440549415315
aHR0cDovL3QueW91bWkubmV0L3YxL2JhdGNoX2V2ZW50
46C02DF8DF4C4C18A578C63449C7F64D
CE94557724F842149D690D0E8CBB1CBD
a13aa5059675e8b8242a7b02292cc6ce
0e1540480e4d1e471a495844580f4c5b041116454509121f550e101742001b14564702
0a4144490c4b1b500e0d0405541b1f4d0714591c0c01111b411507164b47514d005c433c104451004c55
0a4144490c4b1b431003050f16510b44481d5f470f0d4b5a57154[illegible]5018030c004b5a0a011b45005b5b00575612
0a4144490c4b1b500e0d0405541b1f4d0714591c0c01111b45000a0e4b560d114b4f064[illegible]5144
C97CE45F9A5A447c98BBB83D88790503
C6B3C3CCC45547a19B55700AC7C85B9B
555b5f1f185a10080a1b53551d59065[illegible]4534b5b1b4758095e5b5ba3
B77BA25E94FF190AFD2ABAFA[illegible]E2[illegible]7904
0a4144490c4b1b5611[illegible]03104b1b1f5905005e1c0c0[illegible]1b5d0700071618030d1716460f0c515b151658155d5f
0e1540480e4d1e471a495844580f4c5b041116454509121f550e101742001b155b41
a2981b0[illegible]e8df1dcf502f906f97a82
4a45574c6f545557505d3d5d460a5d6b56580812535a15
0a4144490c4b1b56174c1f0b4d580f1a0801441d0d020351404e070d17180e0b174d464d0d40580d
aHR0cDovL3Qu[illegible]YmFsLnl5YXBpLm5ldC92MS9iYXRjaF9ldmVudA==
0e1540[illegible]4d1e471a495844580f4c5b0411165956020f491b000c4b1b440549575f
A33E523A1CEF496dB37ABD886CBCB005
0e1540480e4d1e471a495844580f4c5b041116454509121f550e101742001b055f5d

DD5E8CD46CF94B22BAAD68AB06710752
aca5522945c72310f9f22b333c68f2b3
417e606d53634d5101080a517928555d
4040724c5d4f565a6a42005a622f5d7f
F1B19978F3D74302BA126760F96262CD
0e1540480e4d1e471a495844580f4c5b041116454509121f550e101742001b025a

免责声明及风险提示: